Privacy and Security in the Roman Empire:

One Hospital's Experience with a "Do It Yourself" HIPAA Plan

Melissa Cornwell, HIPAA Coordinator
Floyd Medical Center
Rome, Georgia

What is the Roman Empire?

- Rome, Georgia
- 65 Miles NW of Atlanta, GA
- 65 Miles SW of Chattanooga, TN
- 135 Miles E of Birmingham, AL

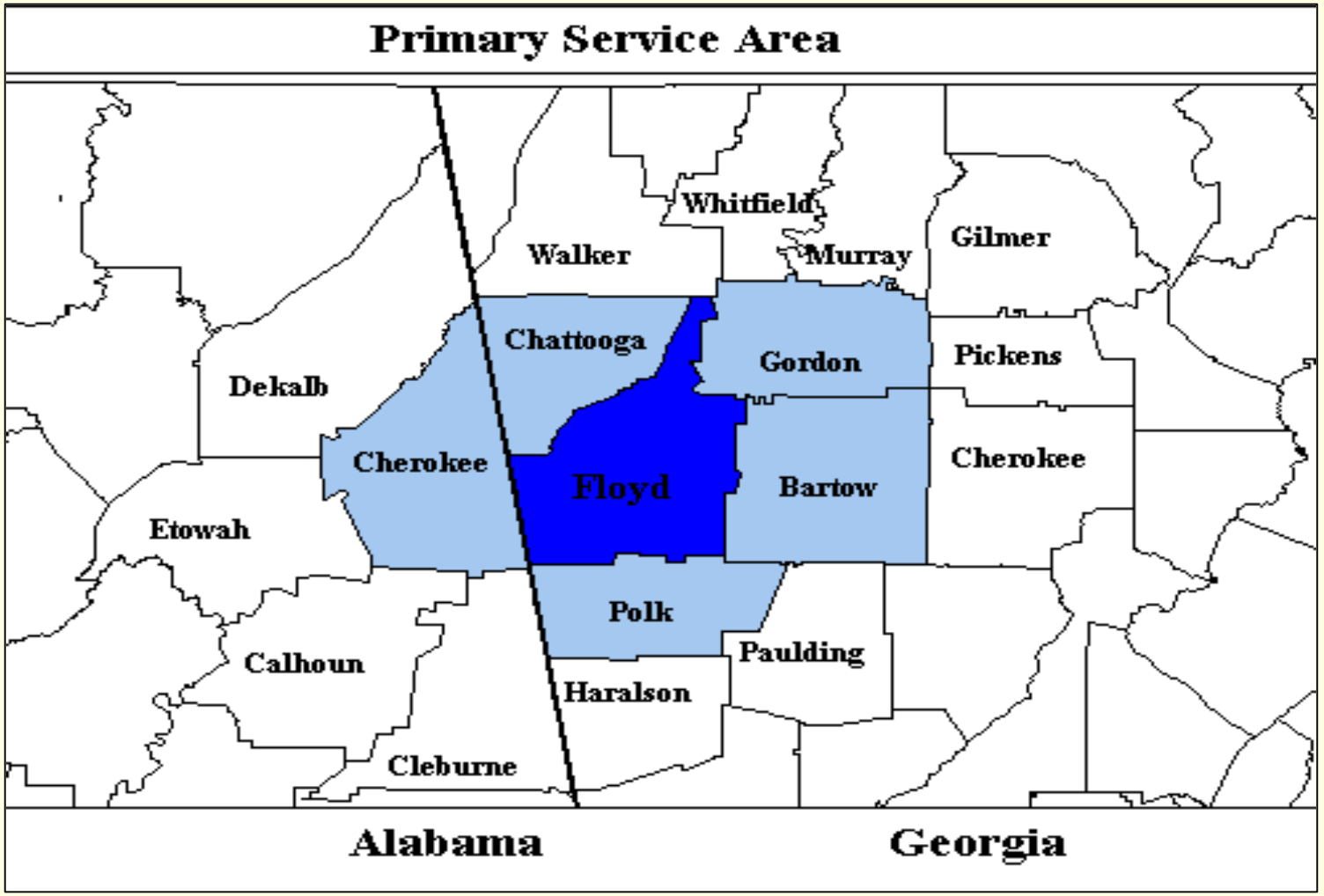
What is the Roman Empire?

- Rome is the county seat of Floyd County, GA
- Rome's Land Area = 22 Square Miles
- Rome's Population = 34,980
- Floyd County Population = 90,565

Rome's Health Care Assets

- Rated #1 in health care out of 193 small cities in the United States, Rome is home to more physicians per capita than any other city in Georgia. We serve as a health care center for a regional population of over 500,000 people (17 North Georgia counties).

Service Area: Floyd Medical Center



Rome's Health Care Assets

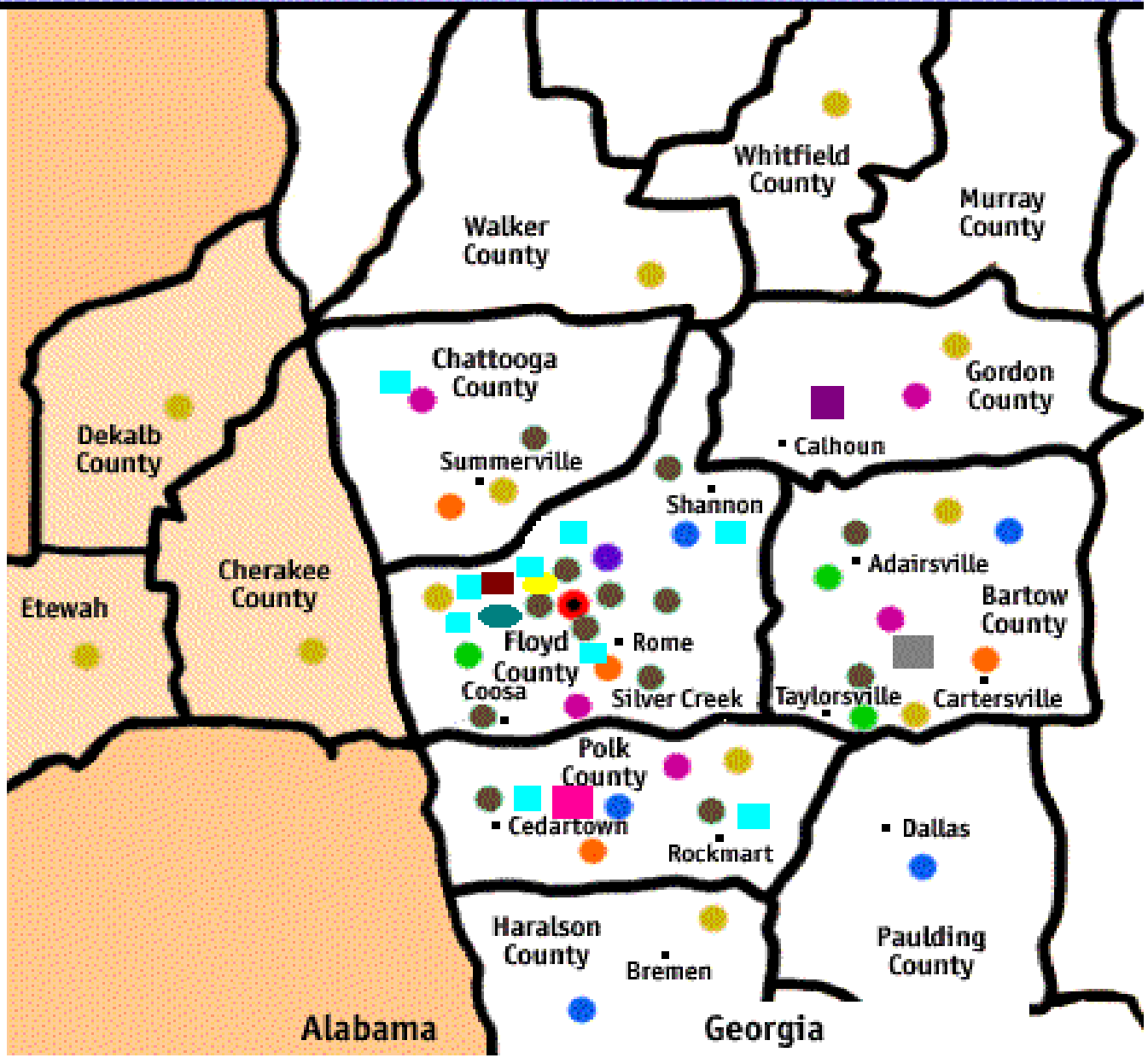
Two Hospitals:

- Floyd Medical Center
  - 304-Bed, Acute Care Hospital
  - Only Women's and Infant Services in Floyd County (maternity, NICU, newborn nursery)
  - Emergency Services
  - Trauma/Intensive Care/Coronary Care
  - Full Medical/Surgical Services
  - Inpatient Rehabilitation Unit
- 201-Bed Acute Care Facility (HCA-owned)
  - Open Heart Surgery Referrals for NW GA

Floyd Medical Center
Rome, GA

Service Area

- Floyd Medical Center
- Centrex Primary Care Offices
- Urgent Care and Occupational Medicine Center
- Community Hospice Care Services
- Floyd Home Health Agency Services
- Windwood Psychiatric Services
- Floyd Rehabilitation Center Services
- The Women's Center
- Columbia Redmond Regional Medical Center
- Redmond Physician Network
- Columbia Polk Medical Center
- Emory Cartersvile Medical Center
- Gordon Hospital
- The Harbin Clinic
- Coosa Clinics



FMC as a “Covered Entity”

- Floyd Medical Center
- Floyd Home Health Agency
- Community HospiceCare
- Centrex Primary Care Network (19 Primary and Urgent Care Offices)
- Windwood Psychiatric Hospital
- Health@work Occupational Health Services
- Floyd Health Care Foundation
- The Women’s Center
- FMC’s Self-Insured Employee Health Plan

FMC's "First Steps for HIPAA"

- Prior to the summer of 2001, two groups within our organization led efforts toward HIPAA compliance:
  - Following a JCAHO survey in January of 2001, the Accreditation Compliance Committee met semi-monthly to discuss privacy-related issues in preparation for a coordinated HIPAA-compliant effort
  - Nursing Informatics led a separate effort toward compliance for the Security Rule and Transactions and Code Sets (TCS) Rule

HIPAA Project Management Office

- **Project Manager: Robbie Lane, a newly retired, thirty-year veteran of our hospital's workforce**
  - Past Director of Medical Records, past Director of Human Resources, and most recently, Senior Director, Case Management/Quality
- **Project Coordinator: Melissa Cornwell, Nursing Project Manager**
  - Previous experience with federal regulations (i.e., HCFA, CARF, Corporate Compliance); policy and procedure development, medical office operations
- **One FTE working on HIPAA since November 5, 2001**

First Tasks

- Read the Regulations
- Identified appropriate and legitimate HIPAA conferences, seminars, and web resources
- Participated in VHA Georgia Compliance/ HIPAA Council meetings
  - Ordered Phoenix Healthcare's audio conference presentation, "Hands-On HIPAA: Developing Your HIPAA Implementation Plan"

The Regulations

- http://aspe.os.dhhs.gov/admnsimp/
  - Downloaded regs in HTML format
  - Copied and pasted into MS Word documents
    - Searchable; original formatting preserved
  - Reviewed other documents on the website:
    - Preamble to the Privacy Rule (4 parts)
    - First Guidance on the Privacy Rule (7/01)
    - HHS Fact Sheets
    - Frequently Asked Questions (FAQ's) documents
  - Subscribed to HIPAA-REGS list for updates

Identifying Resources

BEWARE OF INFORMATION GLUT

FMC's Top Web Resources

- www.hipaadvisory.com
  - Phoenix Health (VHA) site
- www.cpri-host.org/resource/toolkit/toolkit.html
  - Computer-based Patient Record Institute
- http://www.healthlinknm.org/nmchili/
  - New Mexico Coalition for Healthcare Information Leadership Initiatives
- www.clients1.kslaw.com
  - King & Spalding subscription website (Offers Georgia pre-emption information)

FMC’s Top Web Resources

- For more information than you will ever need, go to:

  http://pweb.netcom.com/~ottx4/HIPAA.htm

7 Steps to HIPAA Compliance*

1. Project preparation
2. Develop educational processes including awareness training, instruction re: new HIPAA-compliant policies and procedures, and job-specific training
3. Complete assessment of current practices & subsequent gap analysis
4. Gap closure/implementation
5. Identification of Business Associates & Trading Partners; contract revision/creation
6. Identification of legal issues and solutions
7. Development of ongoing monitoring and auditing

*Adapted from “Hands-On HIPAA: Developing Your HIPAA Implementation Plan” audio conference, copyright Phoenix Healthcare, 2001

Step 1: Project Preparation

- Met with FMC “Sponsors”
  - Senior Vice President
  - Vice President, Corporate Compliance
  - Vice President, Finance
- Selected Privacy Officer
- Selected Security Officer
- Developed Organizational Chart
- Selected HIPAA Compliance Team
- Developed Board Resolution

Step 1: Project Preparation

- Selection of Privacy Officer
  - Director of Health Information Management
- Selection of Security Officer
  - Director of Information Systems/Networking
- Job Descriptions: Duties of Privacy Officer and Security Officer were integrated into existing job descriptions

Step 1: Project Preparation

- Identification of Workgroups
  - Privacy (Chaired by Privacy Officer)
  - Security (Chaired by Security Officer)
  - Transactions & Code Sets (Chaired by Director of Patient Financial Services, with strong workgroup representation from Information Systems/Data Processing)
  - Education Workgroup (Chaired by Director of Corporate Education)

Step 1: Project Preparation

- Appointed a Steering Committee, to include:
  - Sponsors
  - HIPAA Project Management Office
  - Privacy Officer
  - Security Officer
  - Vice Presidents for Nursing, Corporate Operations
  - Human Resources Manager
  - Director of Patient Financial Services
  - Director of Corporate Education

Organizational Structure: HIPAA Compliance Team

Corporate Compliance Committee

HIPAA Sponsors
Sonny Rigas, Sr. V.P.
Mary Johnson, V.P.
Rick Sheerin, V.P.

Legal Counsel

HIPAA Steering Committee
Mary Johnson, Diane Davis, Sonny Rigas, Rick Sheerin, Greg Polley, Robbie Lane, Brian Barnette, Deborah Robitaille, Donna Casey, Linda Wilhelm, Valerie Cloud, Melissa Cornwell

Project Management Office
Robbie Lane, Manager
Melissa Cornwell, Coordinator

Transactions/Code Sets/ Identifiers Workgroup
Donna Casey, Chair

- Rick Sheerin, VP/Designee
- Greg Polley, VP/Designee
- IS Shirley Stafford
- IS Leonard Culberson
- IS Louise McKinney
- IS Renee Brooks
- HIM Deborah Robitaille
- Centrex Anita Borders
- Home Care Carol McBurnett
- Hospice Carol McBurnett
- WW Tara Sherman

Privacy Workgroup
Deborah Robitaille, Privacy Officer
Chair

- Diane Davis, VP/Designee
- IS Renee Brooks
- HR Valerie Cloud
- RM Jackie Newby
- PI Debbie Smith
- Accred Winnie Chesley
- Customer Rel. Denise Martin
- Centrex Al Davis
- Home Care Janice Griffin
- Hospice Janet Elrod
- FP Vicki Wiles
- WW Janette Barker
- HIM Shelley Anderson

Security Workgroup
Brian Barnette, Security Officer
Chair

- IS Stacey Cline
- IS Scotty Harper
- Health Plan Rick Tew
- WW John Minshew
- RM Jackie Newby
- PF Dennis Newby
- Sec Richard Bryant
- Centrex - Al Davis

Education Workgroup
Linda Wilhelm, Chair

- Departmental Educators TBD
- Ed Sherry Payne
- PM Haley Crider
- Additional Members TBD

Step 1: Project Preparation

- Concurrent with development of our organizational chart, we planned project oversight using Microsoft Project
  - Developed an overall HIPAA compliance work plan based on our “7 Steps”
  - Developed separate work plans for each work group
  - Privacy, Security, TCS, and Education work plans were presented only as a suggested framework. Each workgroup is encouraged to use its expertise to mold and perfect the proposed work plan

Step 2: Awareness Training & Education

- Privacy Rule: § 164.530: “A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.”
- Training must be completed by April 14, 2003
- Training must be job specific
- Must train new employees
- Must tailor training as privacy rules change or are updated

Step 2: Awareness Training & Education

- We developed one master set of “HIPAA Basic Training” slides as an early view of the regulations
- Tailored this set for several specific groups:
  - Board of Directors
  - Operations Council
  - Leadership Committee
  - Employees
    - Employee version was included as a 30-minute video segment in our annual Corporate Compliance presentation

Step 2: Awareness Training & Education

- The Education Workgroup is designing and implementing privacy and security training for:
  - New employee orientation
  - Annual employee update
  - Training regarding new policies and procedures
    - We will use our Notice of Privacy Practices as an outline for this training
  - Departmental-based training dependent upon job description and “need to know”

Step 3: Assessment and Gap Analysis

- This is where the fun begins!
- How to assess?
- What to assess?
- Who to assess?
- How to document assessments?
- How to standardize results?
- How to measure gaps?

Step 3: Assessment and Gap Analysis

- Jonathan Tomes, JD: *Compliance Guide to HIPAA and the HHS Regulations*
- Provides a comprehensive list of questions for a HIPAA Privacy Assessment
  - Turns the privacy regs into question format
- We expanded upon that idea and framed three assessments:
  - Privacy
  - Security (based on an AHIMA Model)
  - EDI (based on the regulation text)

Step 3: Assessment and Gap Analysis

- In addition to these rule-specific assessments, we needed an assessment tool that would provide a practical view of current privacy and security practices throughout our organization.

Step 3: Assessment and Gap Analysis

- What do we need to know about our current privacy and security practices that will help us understand our level of compliance with the proposed regulations?
  - Where is protected health information (PHI) entering our systems?
  - Where is PHI exiting our systems?
  - How do our employees use and disclose PHI in their day-to-day work flow?
  - Where is PHI stored?
  - Is stored PHI adequately protected?
  - Who will do the assessments?

Step 3: Assessment and Gap Analysis

- Who will do the assessments?
  - Compliance Team Workgroup members divided into 15 teams of two members each
  - We identified 75 departments requiring assessments
  - Each team was assigned 5 assessments

Step 3: Assessment and Gap Analysis

- Assessment Tool #1 helped us determine:
  - Where is PHI entering our systems?
  - Where is PHI exiting our systems?
  - PHI Mapping Tool

Step 3: Assessment and Gap Analysis

- Assessment Tool #2 provided an answer to the question:
  - What are our current privacy and security practices?
  - Departmental Assessment

Step 3: Assessment and Gap Analysis

- Filling out Assessment Tool #3 was conditional upon answering the last question on Assessment Tool #2, which was, “Do any members of your department store protected health information in any non-clinical programs, or store any paperwork containing PHI?” (Examples: MS Word, Access, Excel, Outlook, 3M, hard copies of patient charts, charge or encounter forms)
- PHI INVENTORY

Step 3: Assessment and Gap Analysis

- Following compilation of departmental assessment results, the Privacy and Security Workgroups are completing “master” assessments
- Those results are being used to complete gap analysis tools

Step 3: Assessment and Gap Analysis

- Gaps are identified by green, yellow and red priorities
  - Green = compliant; little or no risk
  - Yellow = partially compliant; moderate risk
  - Red = non-compliant, high-risk
- Privacy Gap Assessment

Step 4: Gap Closure & Implementation

- "Gap Closure" will be the responsibility of the Compliance Team Workgroups and will include:
  - Development of Notice of Privacy Practices (NPP)
  - Review, revision, and/or creation of privacy and security policies and procedures
  - Review, revision, and/or creation of required and optional forms (consents/authorizations)
  - Security technology purchases/upgrades
  - Dissemination of new policies and procedures
  - Coordination of efforts with Education Workgroup to ensure system-wide education

Step 5: Identification of Business Associates and Contract Development

- Should be a simple task, since Materials Management retains all contracts

Step 5: Identification of Business Associates and Contract Development

- Responses in the departmental assessments showed us that most departments maintain some contracts
- We are conducting a department-by-department inventory of contracts
- Identify those contracts that are currently up for renewal first
- Move forward according to renewal dates
- Current plan is to prepare a standard Business Associate Addendum which includes required verbiage not only for HIPAA, but JCAHO and OIG requirements.

Step 5: Identification of Business Associates and Contract Development

BA	Purpose of Contract	BA Address	Vendor Contact	Contact Phone
Hill-Rom	Purchase/maintenance of patient beds/furnishings	123 High Street, Milwaukee, WI	Jane Doe	232-5326
ABC Staffing	Provide locum tenens staffing	657 Broad Street, Rome, GA	Lamont Dixon	232-8767
Biomed Solutions	Provide biomedical engineering services	345 Sixth Ave., Cartersville, GA	Jay Hight	770-852-2222
IDX	Maintenance of clinical/ billing computer system	234 Sylph St., Ogden, Utah	P.C. Hill	903-222-8787

Step 6: Identification of Legal Issues and Solutions

- What is our status as a “Covered Entity”?
  - Single Covered Entity
  - Hybrid Entity
  - Affiliated Covered Entities
- Review of required documents:
  - Business Associate Agreements
  - Trading Partner Agreements
  - Required forms (authorizations, consents)
  - Policies and Procedures

Step 6: Identification of Legal Issues and Solutions

- How will we establish our Organized Health Care Arrangement?
  - Revision of Medical Staff Bylaws/Rules and Regulations
  - Creation of partnerships with other covered entities with whom we share PHI (MRI facility, angioplasty, etc.)

Step 6: Identification of Legal Issues and Solutions

- Issues for consideration for an OHCA*:
  - Amend staff bylaws to make participation in the OHCA an essential requirement to join or stay on the medical staff
  - Each medical staff member formally agrees to abide by the terms of the notice "with respect to protected health information created or received by the covered entity as part of its participation in the organized health care arrangement." [164.520(d)(1)]

* Issues are adapted from a list compiled by David Hainlain, Citrus Memorial Hospital, and posted in Phoenix Healthcare's HIPAA electronic mail exchange, "HIPAAlive"

Step 6: Identification of Legal Issues and Solutions

- Issues for consideration for an OHCA:
  - The OHCA adopts a single NPP to cover use and disclosure of PHI obtained during the course of treatment while a patient is treated on the premises of the hospital or on material sent for analysis at the hospital's lab.
  - Patient treatment outside of the hospital's premises and not utilizing hospital services, such as a follow-up visit with the surgeon after discharge, is outside the context of the arrangement.

Step 6: Identification of Legal Issues and Solutions

- Issues for consideration for an OHCA:
  - The OHCA agreement acknowledges that the hospital is not responsible for policing other CE's that are members of the OHCA to ensure that they have obtained consent prior to asking for PHI for treatment or payment.
  - The NPP notifies patients that the hospital routinely shares PHI with the medical staff to facilitate treatment by the medical staff to patients and payment to the medical staff for services rendered to the patient in connection to services given to the patient by the hospital.

Step 6: Identification of Legal Issues and Solutions

- Issues for consideration for an OHCA:
  - The OHCA agreement itself must describe:
    - Service delivery sites
    - That members of the OHCA will share PHI for purposes of treatment, payment, and healthcare operations
    - To all members of the OHCA that except for the joint notice, each entity under the OHCA is still a separate entity and responsible for their own HIPAA compliance efforts (transactions, security & privacy).

Step 7: Ongoing Monitoring and Auditing

- Development of policies and procedures which require periodic assessment of privacy practices
- Documentation of privacy and security training
- Inclusion of privacy and security issues in quality review activities
- Built-in monitoring as required by the Security Rule

Cultural Change: The "Soft Side" of HIPAA

- "90% of security violations occur from within the walls of the organization and 90% of those violations occur from personnel who have been granted access to the information for legitimate purposes.

  Ergo – 90% of security lays between the ears – that is training, education, and cultural change management."

  -Tom Hanks, PricewaterhouseCoopers, LLP

Cultural Change: The “Soft Side” of HIPAA

- Cultural change may be the single biggest challenge for covered entities
- Our departmental assessments proved to us that our employees understand the importance of privacy and security in protecting PHI

Cultural Change: The “Soft Side” of HIPAA

- We have come to believe that most breaches in confidentiality are incidental or unintentional
- Constant reinforcement will be required to assure maximum compliance

Cultural Change: The “Soft Side” of HIPAA

- How to strike a balance between customer satisfaction and protection of privacy?
- We base our customer service efforts on the premise that with each client encounter, we automatically think, “How may I help you?”
  - If helping someone involves divulging PHI, how do we tactfully turn down such requests?

Cultural Change: The "Soft Side" of HIPAA

- "The Step Child of HIPAA Compliance: Culture Change" by D'Arcy Guerin Gue
  - "HIPAAtized" culture might be "where compliant attitudes, behaviors and sensitivity to patient privacy and confidentiality become second nature and assumed throughout the workforce."
  - Some believe in the "Field of Dreams" approach to HIPAA Implementation: "Build it and they will come."
    - (i.e., do the assessments, write the policies, institute new technologies, change the forms, schedule the training, and…Voila! The workforce will follow) …maybe

Cultural Change: The "Soft Side" of HIPAA

- Involve employees in the implementation process, especially policy and procedure development
- Use HIPAA implementation as a launching pad for privacy policies and procedures
  - Visitation
  - How to select a "family representative"
  - How to identify individuals who have a "right to know"
  - Chain of command for privacy and security related questions
  - Complaint process

What if it All Goes Away?

- Privacy Rule may be repealed
- Security Rule and Transactions and Code Sets Rules remain (for now)
- Just as you can't have privacy without security, there is no need for security if you are not concerned with privacy
- Policies and procedures will have been created that will only improve our "cultural norm"
- It is still "the right thing to do"